UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/018,605	03/01/2002	Marten De Boer	01819/RPM	5118

1933 7590 02/09/2005

FRISHAUF, HOLTZ, GOODMAN & CHICK, PC
767 THIRD AVENUE
25TH FLOOR
NEW YORK, NY 10017-2023

EXAMINER	
SHIFERAW, ELENI A	
ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 02/09/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 10/018,605	**Applicant(s)** DE BOER ET AL.	
	Examiner Eleni A Shiferaw	**Art Unit** 2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 December 2001*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-9* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-9* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date *12/17/01*.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

1. Claims 1-9 are presented for examination.

Claim Objections

2. Claim 4 is objected to because of the following informalities: Applicant claims claim 4 on line 37 as "also enciphers the then current public key..." the word then needs to be taken out. Appropriate correction is required.

3. Claims 1-9 are objected to because of the following informalities: the abbreviation "TTP" used in the claims has no well-recognized meaning in the field of information processing and leaves the reader in doubt as to the meaning of the technical features to which it refers, thereby rendering the definition of the subject-mater of said claims unclear. Appropriate correction is required.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

5. Claim 1 is rejected under 35 U.S.C. 102(a) as being anticipated by Hewlet Packard Co. (HP, EP 0 892 521 A2)

As per claim 1, Hewlet teaches a system for protectedly storing and managing, in a TTP server, copies of digital files which are transmitted, by way of a transmission channel, from a first to a second user **(HP Col. 17 lines 26-30)**, characterized in that

a file (Txt) is transmitted from the first user (A) to a second user (B) after having been enciphered with a symmetrical session key (SesKey) **(HP Col. 17 lines 26-30)**, which session key is e-enciphered using the public key (PubKeyB) of a first asymmetrical pair of keys (KeyPairB) **(see HP Col. 6 lines 13-21; for use of symmetric key and public key)** associated with the second user, which second user, after having received it, may decipher the session key using the private key (SecKeyB) of said first asymmetrical pair of keys (KeypairB) and subsequently may decipher the file using the session key deciphered in this manner **(HP Col. 17 lines 41-53 and lines 26-30)**, the session key (SesKey) also being enciphered by the first user (A) using the public key (PubKeyTTP) of a second asymmetrical pair of keys (KeyPairTTP) associated with the TTP server **(HP Col. 17 lines 26-30 and col. 18 lines 31-38),** which TTP server, after having received it, deciphers said session key using the private key (SecKeyTTP) from said second asymmetrical pair of keys (KeyPairTTP) **(HP Col. 17 lines 47-53)**, whereafter the TTP server enciphers the deciphered session key (sesKey) using the public key of a third asymmetrical pair of keys (StorKeypair) **(HP Col. 14 lines 58-col. 15 lines 10)**, hereinafter to be referred to as public storage key (PubstorKey), and stores the session key ((sesKey)pubstorKey) enciphered with said storage key, together with the file ((Txt)SesKey) enciphered with the session key (SesKey), in a storage medium (DB) **(HP Col. 13 lines 17-19 and lines 29-41).**

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 2-9 rejected under 35 U.S.C. 103(a) as being unpatentable over Hewlet Packard Co. (HP, EP 0 892 521 A2) in further view of Etzel et al. (Etzel, Patent No.: US 6,577,734 B1)

As per claim 2 HP and Etzel teach all the subject matter as described above. In addition, HP teaches system, characterized in that, periodically, the TTP server deciphers the enciphered file ((Txt)SesKey) stored in the storage medium with the session key (SesKey), which for that purpose is recovered in advance by deciphering the stored enciphered session key (tsesKeylpubstorKey) with the private key of the third pair of keys (StorKeypair), hereinafter to be referred to as the private storage key (SecstorKey) **(HP Col. 6 lines 13-21, col. 13 lines 17-21, and col. 14 lines 49-col. 15 lines 10; file is encrypted by session key, session key is encrypted by receiver's (Long Term Signature Verification or LTSV) public key, and the LTSV decrypts the received file by deciphering the session key in using LTSV's private key**

and LTSV stores data in DB. It is obvious to have another TTL private key to decrypt the session key of the stored data);

the TTP server, comprising a new public storage key (PubstorKey') and a new private storage key (SecstorKey'), and a new version of the symmetrical session key (SesKey'), whereafter the TTP enciphers the deciphered file (Txt) with the new session key (SesKey') and stores the file ((Txt)SesKey') enciphered in this manner in the storage medium (DB) **(HP Col. 6 lines 13-21, col. 13 lines 17-21, and col. 14 lines 49-col. 15 lines 10; session key enciphers the file and the receiver's public key encrypts the session key and the receiver deciphers the file and stores it in the DB. It is obvious to have another set of TTL private storage key, public storage key, and session key to re-encrypt the data with session storage key and encrypt session storage key with public storage key and use private storage key to decrypt because TTL server has more than one client A and B);**

the TTP server enciphers the new session key (SesKey') with the new public storage key (PubstorKey') and stores the session key ((sesKey')pubstorKey') enciphered in this manner in the storage medium (DB) **(HP Col. 14 lines 49-col. 15 lines 10)**.

HP does not explicitly teach subsequently generating a new version of the third pair of keys.

However Etzel teaches generating unique device encryption keys (storage keys) that is never disclosed externally to another device, or unknown to anyone except the device, to encrypt encryption keys and store the keys in local memory, and when retrieving stored encryption keys the device first deciphers the encryption key using unique storage keys (Etzel Col. 1 lines 53-59, and claims 4 and 5).

Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to employ the teachings of Etzel within the system of HP because it would securely manage the encryption keys used in such encrypting to prevent them from being misappropriated for fraudulent purposes (Etzel Col. 1 lines 47-50).

As per claim 3, HP and Etzel teach all the subject matter as described above. In addition HP discloses system, characterized in that, for protected recovery of the file (Txt) and transmission thereof to the first user (A) or the second user (B) **(HP Col. 17 lines 26-30)**, as the case may be, the symmetrical session key (SesKey) is recovered from the storage medium by deciphering, with the private storage key (SecstorKey) **(HP Col. 6 lines 13-21; decrypting session key with private key)**, the stored enciphered session key ((SesKey) PubstorKey), whereafter the recovered session key (SesKey) is subsequently enciphered with the current public key (PubKeyA' or PubKeyB, as the case may be) of the first or second user (A or B, as the case may be) **(HP Col. 6 lines 13-21; encrypting session key by public key of the receiver)**, and is transmitted to the user by way of the transmission channel, together with a copy of the file ((Txt)SesKey) stored in the storage medium **(HP Col. 15 lines 44-53; LTSV Verifies digital signature to client A and B over the transmission channel)**, with the user, after having received the enciphered session key ((SesKey)PubKeyA' or (SesKeylpubKeyB', as the case may be), being capable of recovering the session key therefrom by deciphering using the user's private key (SecKeyA' or SecKeyB': as the case may be), and subsequently being capable of deciphering the enciphered file ((Txt)SesKey) using the recovered session key **(HP Col. 17 lines 37-47).**

Etzel teaches generating unique device encryption keys (storage keys) that is never disclosed externally to another device, or unknown to anyone except the device, to encrypt encryption keys and store the keys in local memory, and when retrieving stored encryption keys the device first deciphers the encryption key using unique storage keys (Etzel Col. 1 lines 53-59, and claims 4 and 5). The rational for combining are the same as claim 2 above.

As per claim 4 HP and Etzel teach all the subject matter as described above. In addition HP discloses system, the public key (PubKeyA) of the first user (A) being used to verify a digital signature (DigSign) of the file (Txt), characterized in that the TTP Server **(HP Col. 18 lines 45-col. 19 lines 10)**, after having received the enciphered file ((Txt)SesKey), also enciphers the then current public key (PubKeyA) of the first user (A) using the public storage key (PubstorKey), and stores said enciphered public key ((PubKeyA)PubStorKey) in the storage medium (DB) (HP Col. 14 lines 49-col. 15 lines 10).

Etzel teaches generating unique device encryption keys (storage keys) that is never disclosed externally to another device, or unknown to anyone except the device, to encrypt encryption keys and store the keys in local memory, and when retrieving stored encryption keys the device first deciphers the encryption key using unique storage keys (Etzel Col. 1 lines 53-59, and claims 4 and 5). The rational for combining are the same as claim 2 above.

As per claim 5 HP and Etzel teach all the subject matter as described above. In addition HP discloses system, characterized in that, the TTP server deciphers the enciphered public key (PubKeyA) of the first user stored in the storage medium with the private storage key

(SecstorKey) **(HP Col. 6 lines 13-21, col. 13 lines 17-21, and col. 14 lines 49-col. 15 lines 10; file is encrypted by session key, session key is encrypted by receiver's (Long Term Signature Verification or LTSV) public key, and the LTSV decrypts the received file by deciphering the session key in using LTSV's private key and LTSV stores data in DB. It is obvious to have another TTL private key to decrypt the session key of the stored data)**;

the TTP server, comprising a new public storage key (PubstorKey') and a new private storage key (SecstorKey') **(HP Col. 6 lines 13-21, col. 13 lines 17-21, and col. 14 lines 49-col. 15 lines 10; session key enciphers the file and the receiver's public key encrypts the session key and the receiver deciphers the file and stores it in the DB. It is obvious to have another set of TTL private storage key, public storage key, and session key to re-encrypt the data with session storage key and encrypt session storage key with public storage key and use private storage key to decrypt because TTL server has more than one client A and B)**;

the TTP server enciphers the deciphered public key (PubKeyA) of the first user with the new public storage key (PubstorKey') and stores said public key (PubKeyA)PubStorKey'), enciphered in this manner, in the storage medium **(HP Col. 14 lines 49-col. 15 lines 10)**.

Etzel teaches generating unique device encryption keys (storage keys) that is never disclosed externally to another device, or unknown to anyone except the device, to encrypt encryption keys and store the keys in local memory, and when retrieving stored encryption keys the device first deciphers the encryption key using unique storage keys (Etzel Col. 1 lines 53-59, and claims 4 and 5). The rational for combing are the same as claim 2 above.

As per claim 6 HP and Etzel teach all the subject matter as described above. In addition HP discloses system, characterized in that the public key (PubKeyA) of the first user is recovered from the storage medium by deciphering, with the private storage key (SecstorKey) **(HP Col. 17 lines 37-50; LTSV decrypts the public key of the first client)**, the stored enciphered public key ((pubKeyAlpubstorKey) of the first user, that said original public key (PubKeyA) recovered in this manner is subsequently enciphered with the current public key (RthKeyA') or PubKeyB', as the case may be) of the first or second user (A or B, as the case may be), and is transmitted by way of the transmission channel to the first or second user **(HP Col. 6 lines 13-21; encrypting a key using receivers public key and transmitting it to the receiver)**, as the case may be, with the user, after having received said enciphered public key (PubKeyA)PubKeyA' or (PubKeyA)PubKeyB', as the case may be) being capable of recovering the original public key (PubKeyA) of the first user therefrom by deciphering with his current private key (SecKeyA' or SecKeyB', as the case may be) **(HP Col. 6 lines 13-21; receiver deciphers the key using receivers private key)**, and subsequently being capable of verifying the digital signature (DigSign) of the file (Txt) using the original public key (PubKeyA) of the first user recovered in this manner **(HP Col. 18 lines 45-col. 19 lines 10)**.

Etzel teaches generating unique device encryption keys (storage keys) that is never disclosed externally to another device, or unknown to anyone except the device, to encrypt encryption keys and store the keys in local memory, and when retrieving stored encryption keys the device first deciphers the encryption key using unique storage keys (Etzel Col. 1 lines 53-59, and claims 4 and 5). The rational for combing are the same as claim 2 above.

As per claim 7 HP and Etzel teach all the subject matter as described above. In addition HP discloses system, characterized in that the digital signature (Digsign) is enciphered with the current public key (PubKeyA) or (PubKeyB), as the case may be) of the first or second user (A or B, as the case may be), and is transmitted to said first or second user, as the case may be, whereafter the receiving user recovers the digital signature by deciphering the received, enciphered digital signature ((DigSign)PubKeyA' or (DigSign)PubKeyB', as the case may be) with his private key (SecKeyA' or SecKeyB', as the case may be) **(HP Col. 7 lines 49-col. 8 lines 26)**.

Etzel teaches generating unique device encryption keys (storage keys) that is never disclosed externally to another device, or unknown to anyone except the device, to encrypt encryption keys and store the keys in local memory, and when retrieving stored encryption keys the device first deciphers the encryption key using unique storage keys (Etzel Col. 1 lines 53-59, and claims 4 and 5). The rational for combing are the same as claim 2 above.

As per claim 8 HP and Etzel teach all the subject matter as described above. In addition HP discloses system, characterised in that the TTP server, after having received the enciphered file (lTxtlsesKey) generates a time stamp (TStamp) **(HP Col. 15 lines 44-53)** and stores it, linked to the stored file and enciphered with the public storage key (PubstorKey), in the storage medium (DB) **(HP Col. 17 lines 1-10)**.

Etzel teaches generating unique device encryption keys (storage keys) that is never disclosed externally to another device, or unknown to anyone except the device, to encrypt encryption keys and store the keys in local memory, and when retrieving stored encryption keys the device first deciphers the encryption key using unique storage keys (Etzel Col. 1 lines 53-59, and claims 4 and 5). The rational for combing are the same as claim 2 above.

As per claim 9 HP and Etzel teach all the subject matter as described above. In addition HP discloses system, characterized in that, in the event of retrieving the stored file by the first or second user (A or B, as the case may be) the enciphered time stamp ((Tstamp)pubstorKey) is recovered by deciphering with the private storage key (SecstorKey) **(HP Col. 16 lines 28-42),** the recovered time stamp is subsequently enciphered with the current public key (PubKeyA) or PubKeyB', as the case may be) for the querying user, and is transmitted to said user. whereafter the user may decipher the enciphered time stamp ((TStamp)PubKeyA' or (TStamp)PubKeyB', as the case may be) with the private key (SecKeyA' or SecKeyB', as the case may be) current for said user **(It is obvious to one skilled in the art at the time of the invention was made to decipher the timestamp in using TTL private storage key and encrypt the deciphered timestamp with the receivers public key because, HP Col. 6 lines 13-21, discloses a user encrypting a session key in using receivers public key and when the receiver receives it, decrypting the session key to read the file using receivers private key).**

Etzel teaches generating unique device encryption keys (storage keys) that is never disclosed externally to another device, or unknown to anyone except the device, to encrypt encryption keys and store the keys in local memory, and when retrieving stored encryption keys the device first deciphers the encryption key using unique storage keys (Etzel Col. 1 lines 53-59, and claims 4 and 5). The rational for combing are the same as claim 2 above.

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Eleni A Shiferaw whose telephone number is 571-272-3867. The examiner can normally be reached on Mon-Fri 8:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Eleni Shiferaw

Art Unit 2136
January 28, 2005

KIM VU
PERVISORY PATENT EXAM
TECHNOLOGY CENTER 2